



Using Google[™] as a Reconnaissance Tool

“Google is in many ways (the) most dangerous website on the Internet....”

- Scott Granneman, *SecurityFocus*



The problem isn't new...

[The Register](#) » [Internet and Law](#) »

Crackers use search engines to exploit weak sites

By [Thomas C Greene in Washington](#)

Published Sunday 25th June 2000 12:19 GMT

The Problem of Search Engines and "Sekrit" Data
Posted by [Hemos](#) on Mon Nov 26, '01 11:43 AM
from the how-to-choose-data dept.
Nos. writes: "[CNet](#) is *reporting* that not only [Google](#) but other search engines are finding password and credit card numbers while doing



...but it persists,...

Google Hacking Database: Entries by Category

**Advisories and
Vulnerabilities (78)**

Error Messages (54)

**Files containing juicy
info (192)**

**Files containing
passwords (96)**

**Files containing
usernames (13)**

Sensitive Online

Shopping Info (7)

Vulnerable Files (33)

Vulnerable Servers (37)

**Web Server Detection
(54)**

Footholds (11)

**Pages containing login
portals (106)**

**Pages containing
network or vulnerability
data (42)**

Sensitive Directories (48)



...even evolves and grows.

Selected Online Devices (76) accessible to anyone:

- "Copyright (c) Tektronix, Inc." "**printer status**"
- "intitle:Cisco Systems, Inc. **VPN 3000 Concentrator**"
- "powered by **webcamXP**" "Pro|Broadcast"
- intitle:"**Spam Firewall**" inurl:"8000/cgi-bin/index.cgi"
- intitle:"SpeedStream **Router Management Interface**"
- inurl:**TiVoConnect**?Command=QueryServer
- Xerox Phaser® 840 **Color Printer**

Who/What is to Blame?

The Google?

- Easy to use
- Free
- Fast
- Global coverage
- Safe (no trail)

Google Advanced Search Operators

site: search for references to the specified site

link: find sites containing search term as a link

cache: display the cached version of pages found

intitle: find sites containing terms in the title of a page

inurl: find sites containing terms in the URL of a page

filetype: search specific document types



Advanced Search in Google

Google

Advanced Search

[Advanced Search Tips](#) | [About Google](#)

[Web](#) [Images](#) [Groups](#) [News](#) [more »](#)

inurl:"google hack"

Search

[Advanced Search](#)
[Preferences](#)

Search: ☒ the web ☐ pages from Canada

Web

Results 11 - 20

hack" (0.10 sec

e.g.
"exploit"

"b"

any format
any format
Adobe Acrobat PDF (.pdf)
Adobe Postscript (.ps)
Microsoft Word (.doc)
Microsoft Excel (.xls)
Microsoft Powerpoint (.ppt)
Rich Text Format (.rtf)

anywhere in the page

e.g. google.com, .org [More info](#)

anytime
anytime
past 3 months
past 6 months
past year

GDS - <http://gd.tuwien.ac.at/g/go/google-hack/>

Goodie Domain Service offers Open Source Software
for the Austrian Educational Community.

sf.gds.tuwien.ac.at/g/go/google-hack/ - 15k - [Cached](#) - [Similar pages](#)

Occurrences

Return results where my terms occur

Domain

Only return results from the site or domain

SafeSearch

☒ No filtering ☐ Filter using [SafeSearch](#)

Only vs.
Don't

Who/What is to Blame?

Security Analysts?

- Reveal vulnerabilities
- Discuss exploits
- Make attacks newsworthy

SecurityFocus BUGTRAQ Vulns exploit: Google Desktop Search Remote Information Disclosur - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.securityfocus.com/bid/12052/exploit/

Getting Started Latest Headlines Google BMD RBC

Home Foundations Microsoft UNIX IDS Incidents Virus Pen-Test Firewalls Bugtraq

Vulnerabilities Library Calendar Tools Service Vendors Security Jobs Product Search

VULNERABILITIES

Google Desktop Search Remote Information Disclosure Vulnerability

info discussion exploit solution credit help

Currently we are not aware of any exploits for this issue. If you feel we are in error or are aware of more recent information, please mail us at: vulldb@securityfocus.com <mailto:vulldb@securityfocus.com>.

Disclaimer | About The Vulnerability Database

For additions or corrections please email vulldb@securityfocus.com

Who/What is to Blame?

Hackers

Prodigie ?

**Smart
operators**

Script Kiddies

SKILLS

Knowledge

- **Politics**
- **Financial gain**
- **Status**
- **Challenge**
- **Vandalism**

MOTIVES

• **Detect vulnerability**

• **Devise exploit**

• **Test & tune exploit**

Disseminate

• **Use**

ACTIONS

exploits

Who/What is to Blame?

Source: Symantec. All data for Jan-June
2004

SysAdmins?

- 48 new vulnerabilities/week
- 5.8 days from vuln. disclosure to an exploit
- 70% easy to exploit
- 39% associated with Web application tech.
- poor training, resources

Industry?

- ever new software
- rush to market
- lack of testing

Government?

- regulatory framework?
- problem: *dual purpose tools* (like guns): defensive-offensive

The Problem Revisited

A Routine Problem?

source of vulnerability

- INFOSEC ANALYST: disclosure
- SYSADMIN: ignores/neglects
- HACKER: finds out; explores; creates exploitation tools...
- GOOGLE: confirms problem, paves the way to it's exploitation

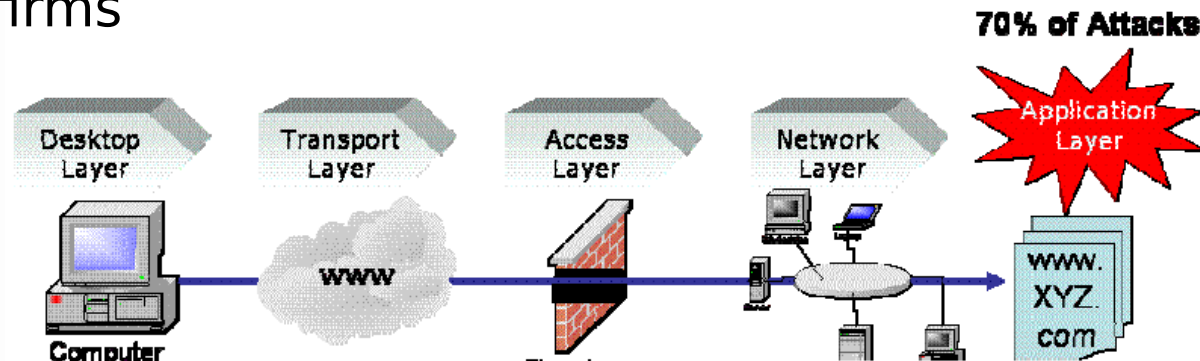
“Distributed responsibility”?



A Deeper Problem?

and at “network layer” attacks

- However, “application layer” attacks increasing in prevalence
- Training and awareness of rising importance
- Technology-alone will fail



Source: SPI Labs

Counter-measures

Passive

- Keep sensitive data off the web!
- Remove site or pages from search engine's index.
- Prevent access to devices (printers, cameras, copiers) from Web applications, or use proven access control measures

Active

- “Google” the site(s) for vulnerabilities.
- Use Foundstone's SiteDigger, or similar tool, to check for vulnerabilities
- Keep track of newly disclosed (“dynamic”) vulnerabilities
- Train the workforce in active measures

Conclusions

Not just Google, but Google the most popular

Pros

- Easy
- Free
- Fast
- Global
- Safe



Cons

- Imprecise, “shotgun-like” tool
- Complementary to other tools, rather than a substitute



Questions?

anton.ljutic@cse-cst.gc.ca